



REC'D	31 NOV 2004
WIPO	PCT

MAGYAR KÖZTÁRSASÁG

ELSŐBBSÉGI TANÚSÍTVÁNY

Ügyszám: P0400489

A Magyar Szabadalmi Hivatal tanúsítja, hogy

Jobbágy Miklós, Kecskemét,
Kuti Gábor, Jászberény,
Zelenák János, Budapest,

Magyarországon

2004. 03. 01. napján 7043/04 iktatószám alatt,

Eszközkészlet közvetlen információ-forgalom interneten keresztül történő biztonságos lebonyolítására

című találmányt jelentett be szabadalmazásra.

Az idefűzött másolat a bejelentéssel egyidejűleg benyújtott melléklettel mindenben megegyezik.

Budapest, 2004. év 11. hó 12. napján

A kiadmány hitelül: Szabó Emilné osztályvezető-helyettes

The Hungarian Patent Office certifies in this priority certificate that the said applicant(s) filed a patent application at the specified date under the indicated title, application number and registration number. The attached photocopy is a true copy of specification filed with the application.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)



Eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására

A találmány tárgya eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására, amely információ továbbító hálózattal történő együttműködésre alkalmas, az információ-forgalomban résztvevő információ közvetítő végkészülékeket tartalmaz, az egyes információ közvetítő végkészülékek küldő részegységgel és fogadó részegységgel, valamint készülékazonosító jelzést tartalmazó ID-regisztert, kódoló kulcs tárolására alkalmas C-regisztert és dekódoló kulcs tárolására alkalmas D-regisztert magukban foglaló tároló részegységgel vannak ellátva, ahol a kódoló kulcsot tartalmazó C-regiszter a küldő részegységgel van összeköttetésben, az egyes információ közvetítő végkészülékekhez pedig kódoló kulcs és azzal együttműködő dekódoló kulcs van hozzárendelve.

A technika, ezen belül a számítástechnika és a telekommunikáció fejlődésével egyre szélesebb körben terjednek el az elektronikai eszközök segítségével megvalósítható hang- és egyéb jelátviteli megoldások. Ezek egy részénél nem a szokásos nyilvános távbeszélő hálózatokat használják, sőt adott esetben, pl. banki információk továbbítására és tranzakciók lebonyolítására a forgalmazott adatokat kódolják, titkosítják is.

A WO 00/41383 közzétételi számú nemzetközi bejelentés olyan megoldást ismertet, amelynek segítségével két telefonkészülék között megfelelő telefonalközpont megléte esetén úgy építhetik föl a kommunikációs láncot, hogy a hívás kezdeményezése után az alközpont vezérlőegysége elsőként egy telefonszámokat és Internet címeket párosító távoli hozzáférésű adatbázist keres föl, ott megpróbálja megtalálni a hívott telefonszámot, és ha azt azonosítani tudja, akkor a telefonszámhoz kapcsolódó Internet címet kiolvassza, a kapcsolatot nem a nyilvános telefonhálózaton keresztül, hanem az Interneten át építi föl, ha ilyen telefonszám-Internet azonosító kapcsolatot nem talál, akkor a hívást a szokásos nyilvános telefonhálózaton keresztül valósítja meg.

A megoldás hátránya azonban, hogy ha a tárcsázott telefonszámhoz nem létezik Internet elérés, akkor az összeköttetést a szokásos módon, a nyilvános telefonhálózaton át hozza létre, ami a hívó fél számára mindenképpen költséget okoz.

További hátrány, hogy a költségkímélő megoldás a hívó és hívott fél Internet elérhetősége mellett mindenképpen igényli még a hagyományos telefonkapcsolat meglétét, sőt egy-egy sajátos telefonalközpont telepítését, ami jelentős beruházási költségnövekedéssel jár, valamint további üzemeltetési és karbantartási kiadásokat is megkövetel.

Jelentős hátránya a megoldásnak még az is, hogy az adatforgalmi kapcsolat titkosítása nincs megoldva, és így a forgalom lehallgatható, nem jogosult harmadik fél számára könnyen hozzáférhető, ezáltal a felépített jeltovábbító vonal nem használható föl tetszőleges tartalommal bíró adatok közvetítésére.

A WO99/62222 közzétételi számú nemzetközi bejelentésben foglalt másik megoldás a telefonforgalom titkosítására vonatkozik. Lényege, hogy az egyes felhasználók saját jelszót kapnak, amelyet bejelentkezésük után minden esetben meg kell adjanak a központi egység számára, saját azonosításuk céljából. Az azonosított felhasználó olyan időintervallumhoz kötött hozzáférési időt kap a központtól, amely időtartam alatt az adatforgalma titkosan zajlik.

Ezen megoldás legnagyobb hátránya azonban, hogy a titkosított adatforgalom időtartama időben korlátozott, ami hosszabb kapcsolati igény esetében lényegében kizárja a bizalmas információátadás lehetőségét.

További hátrány az is, hogy ebben az esetben a felhasználónak saját magának kell bejelentkeznie a rendszerbe, majd egy számára megadott, és így mások által is megismerhető jelszót kell megküldenie a központi egységnek, ami a mások számára is hozzáférhető jelszó használatának lehetősége miatt bizonytalanná teszi a bizalmas adatforgalom bonyolítását, és azt, hogy ezen csatornát kizárólag egy adott készülék vagy felhasználó vehesse igénybe.

Az előzőekből következően a találmánnyal célunk az ismert megoldások hiányosságainak kiküszöbölése és olyan eszközkészlet megalkotása volt, amelynek segítségével a szokásos telefonálással megegyező módon lehet hang-, jel- vagy egyéb adatforgalmat lebonyolító összeköttetést létesíteni két vagy több távoli előfizető között úgy, hogy a kapcsolat időigényétől függetlenül, annak teljes időtartama alatt titkos információforgalmat tegyen lehetővé, és a használat minden esetben a biztos használati költséggel járó nyilvános telefonhálózat megkerülésével internetes vonalon történhessen meg.

A találmányi gondolat alapját az a felismerés képezte, hogy ha egy alkalmasan kialakított központi számítástechnikai egységet és azzal Internet-alapú kapcsolat létesítésére alkalmas végkészülékeket az ismertektől eltérő módon látunk el kódoló és dekódoló kulcsokkal, akkor kialakítható olyan helyzet, amelyben Internetes alapú kommunikáció valósítható meg amellet, hogy az egymással összekapcsolódó hívó és hívott fél hang-, álló vagy mozgókép-, jel- vagy egyéb adatforgalma az összeköttetés megkezdésétől, annak végéig visszafejthetetlenül titkos módon történik úgy, hogy a rendszer használói nem rendelkeznek semmilyen eltulajdonítható titkosító kulccsal vagy jelszóval, ami a hálózat integritását veszélyeztethetné, továbbá a központi számítástechnikai egység önmagában alkalmas a végkészülékek kommunikációjának felügyeletére és menedzselésére, és így a feladat megoldható.

A kitűzött célnak megfelelően a találmány szerinti eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására, - amely információ továbbító hálózattal történő együttműködésre alkalmas, az információ-forgalomban résztvevő információ közvetítő végkészülékeket tartalmaz, az egyes információ közvetítő végkészülékek küldő részegységgel és fogadó részegységgel, valamint készülékazonosító jelzést tartalmazó ID-regisztert, kódoló kulcs tárolására alkalmas C-regisztert és dekódoló kulcs tárolására alkalmas D-regisztert magukban foglaló tároló részegységgel vannak ellátva, ahol a kódoló kulcsot tartalmazó C-regiszter a küldő részegységgel van összeköttetésben, az egyes információ közvetítő végkészülékekhez pedig kódoló kulcs és azzal együttműködő dekódoló kulcs van hozzárendelve – oly módon van kialakítva, hogy minden egyes információ közvetítő végkészülék tároló részegysége más információ közvetítő végkészülékek kódoló kulcsainak ideiglenes tárolására szolgáló egy vagy több átmeneti tároló regiszterrel, míg az információ továbbító hálózat legalább egy központi forgalomkoordináló egységgel van kiegészítve, a központi forgalomkoordináló egységnek mester-dekódoló kulcsot tároló MD-regisztere, valamint az egyes információ közvetítő végkészülékekhez tartozó kódoló kulcsok tárolására szolgáló alapekeszeket tartalmazó memóriaegysége van, továbbá a központi forgalomkoordináló egységhez a mester-dekódoló kulccsal együttműködő mester-kódoló kulcs van hozzárendelve, az információ közvetítő végkészülékek C-regiszterei pedig a központi forgalomkoordináló egység MD-regiszterében tárolt mester-dekódoló kulccsal együttműködő mester-kódoló kulccsal vannak ellátva.

A találmány szerinti eszközkészlet további ismérve lehet, hogy az információ közvetítő végkészülékek átmeneti tároló regiszterei a küldő részegységgel vannak kapcsolatban.

Az eszközkészlet egy lehetséges kialakításánál a központi forgalomkoordináló egység mesterkódoló kulcsot tároló MC-regiszterrel van ellátva.

A találmány ismét eltérő megvalósításánál az egyes információ közvetítő végkészülékek tároló részegységében csak az adott információ közvetítő végkészülék saját kódoló kulcsától mentes információk vannak elhelyezve.

A találmány szerinti eszközkészlet legnagyobb előnye, hogy alkalmazása esetén a hívó és hívott fél közötti kapcsolatfelvétel egyszerű eszközökkel, a hagyományos telefonhasználatnál megszokott módon történhet meg, de az információáramlás költségei lényegesen kedvezőbbek, az adattartalom áramlása viszont a kapcsolat teljes időtartama alatt garantáltan titkos marad.

Előnynek kell tekinteni azt is, hogy az eszközkészlethez tartozó információ közvetítő végkészülék megléte esetén nincs szükség további költséges kiegészítő elemek beszerzésére, működtetésére vagy karbantartására, ami a használattal kapcsolatos kiadásokat befolyásolja kedvezően.

Ugyancsak előnynek kell tekinteni, hogy a sajátos felépítésű információ közvetítő végkészülék a központi forgalomkoordináló egységgel együtt önmagában valósítja meg az adatforgalom titkosítását, így nincs szükség a felhasználóknak kiadott – és így jogosulatlan személyek részére is hozzáférhető – kódra, azonosítóra vagy egyéb kiegészítő kulcsra. Ebből következő előny az is, hogy nem fordulhat elő olyan eset sem, amelyben a felhasználó azért nem tud bekapcsolódni a rendszer működésébe, mert elfelejtette saját kódját.

A találmány további kedvező tulajdonsága még az is, hogy a két végpont közötti adatforgalom végső soron nem egy központon keresztül történik meg, ami gyorsítja az információáramlást, továbbá tovább javítja a rendszer biztonságát, az adatok visszafejthetetlenségét és lehallgathatatlanná teszi a rendszert.

Az előnyök között kell megadni azt is, hogy a találmány szerinti eszközkészlet sajátosságából adódóan a végkészülékek a központi számítástechnikai egység megkerülés esetén használhatatlanná válnak, ami megalapozza azt, hogy a végkészülékek felhasználói csak a központi számítástechnikai egységet üzemeltető jóváhagyásával léphessenek be a rendszerbe.

Az is az előnyök közé sorolható, hogy az eszközkészlet a végkészülékek és a központi számítástechnikai egység adott üzemeltető által történő kódoló-dekódoló kulcspárokkal való feltöltés esetén a gyártótól függetlenül hozható működőképes állapotba, és így olyan zárt hálózat alakítható ki, amely csak bizonyos felhasználók körének teszi lehetővé a kommunikációt.

A találmány szerinti eszközkészletet a továbbiakban kiviteli példa kapcsán, rajz alapján ismertetjük részletesebben. A rajzon az

1. ábra a találmány szerinti eszközkészlet elemeinek vázlatos elrendezési képe.

Az 1. ábrán a találmány szerinti eszközkészlet egy olyan változata látható, amelynél – az egyszerűség kedvéért – csak egy darab hívást kezdeményező 10 információ közvetítő végkészüléket és egy darab hívást fogadó 20 információ közvetítő végkészüléket részleteztünk. Nyilvánvaló azonban, hogy az eszközkészletnek tetszőleges számú 10 információ közvetítő végkészülék lehet része. A 10 információ közvetítő végkészülékek mennyiségének csak a 40 központi forgalomkoordináló egység kapacitása szab határt.

A 10 információ közvetítő végkészülék és a 20 információ közvetítő végkészülék közötti kapcsolatot a 30 információ továbbító hálózat valósítja meg, a 40 központi forgalomkoordináló egység segítségével. A 30 információ továbbító hálózat tetszőleges kommunikációs hálózat lehet, ami ebben az esetben vezetékes és vezeték nélküli, privát és nyilvános hálózatot egyaránt jelenthet. A 30 információ továbbító hálózattal szemben támasztott egyetlen követelmény, hogy alkalmas legyen a továbbítandó jeleknek a telekommunikációban megszokott nagysebességű és lehetőleg torzításmentes átvitelére.

Az 1. ábrán látható, hogy a 40 központi forgalomkoordináló egység lényegében egy olyan nagyteljesítményű számítástechnikai eszköz, amely egyfelől rendelkezik a 41 MC-regiszterrel, a 42 MD-regiszterrel, másfelől tartalmazza a 43 memóriaegységet. A 41 MC-regiszterben helyezkedik el a 41a mester-kódoló kulcs, míg a 42 MD-regiszterben a 42a mester-dekódoló kulcs. Ezen egyedi kulcs-pár teszi lehetővé, hogy a 10 információ közvetítő végkészülék és a 20 információ közvetítő végkészülék titkosított adatforgalmat bonyolíthasson le a 40 központi forgalomkoordináló egységgel. A 40 központi forgalomkoordináló egység 43 memóriaegységében pedig olyan 43a alaprekesz és 43b alaprekesz található, amelyekben a 10 információ közvetítő végkészülék 16 kódoló kulcsa, a 20 információ közvetítő végkészülék 26 kódoló kulcsa található meg rezidens módon.

Itt kell megemlíteni azonban, a 41a mester-kódoló kulcsnak és az azt tartalmazó 41 MC-regiszternek nem szükségszerű a 40 központi forgalomkoordináló egységben lennie. A 41 MC-regiszter és a 41a mester-kódoló kulcs elhelyezhető a 40 központi forgalomkoordináló egységtől távol is úgy, hogy a 41a mester-kódoló kulcs és a 42a mester-dekódoló kulcs ne legyen egy helyen hozzáférhető.

A 10 információ közvetítő végkészülék a hagyományos telefonkészülékeknél megszokott – de itt nem is jelölt – billentyűzet, mikrofon és hangsugárzó mellett rendelkezik még a 11 tároló részegységgel, a 18 küldő részegységgel, és a 19 fogadó részegységgel. A 11 tároló részegységhez tartozik a 12a készülékazonosító jelzés rögzítésére szolgáló 12 ID-regiszter, a 10 információ közvetítő végkészülék saját 17 dekódoló kulcsát tartalmazó 14 D-regiszter. Ide tartozik még a 40 központi forgalomkoordináló egység 41a mester-kódoló kulcsának ideiglenes vagy állandó tárolására alkalmas 13 C-regiszter, továbbá a 15 átmeneti tároló regiszter is, amely az aktuális adatforgalmat bonyolító másik végkészülék – esetünkben a 20 információ közvetítő végkészülék – 26 kódoló kulcsának a kapcsolat alatti tárolását oldja meg. Célszerű, ha a 10 információ közvetítő végkészülék 15 átmeneti tároló regisztere a 18 küldő részegységgel van kapcsolatban.

A 20 információ közvetítő végkészülék szerkezeti felépítése gyakorlatilag megegyezik a 10 információ közvetítő végkészülékével. Itt is megtalálható a hagyományos telefonkészülékeknél megszokott – és itt ugyancsak nem ábrázolt – billentyűzet, mikrofon és hangsugárzó, továbbá a 21 tároló részegység, a 28 küldő részegység és a 29 fogadó részegység. A 21 tároló részegységhez tartozik a 22 ID-regiszter, a 23 C-regiszter, a 24 D-regiszter és a 25 átmeneti tároló regiszter. A 22 ID-regiszter feladata, hogy a 20 információ közvetítő végkészülék egyedi jelzését nyújtó 22a készülékazonosító jelzését rögzítse, míg a 24 D-regiszteré, hogy a 20 információ közvetítő végkészülék saját 27 dekódoló kulcsát hordozza. A 25 átmeneti tároló regiszterben az éppen kapcsolatban lévő – esetünkben a – 10 információ közvetítő végkészülék 16 kódoló kulcsa található meg ideiglenesen. A 23 C-regiszter pedig itt is a 41a mester-kódoló kulcs ideiglenes vagy végleges tárolására szolgál. A 20 információ közvetítő végkészülék szempontjából előnyös, ha a 25 átmeneti tároló regiszter a 28 küldő részegységgel van összeköttetésben.

Az eszközkészlet működésének egy lehetséges megvalósítása során a 10 információ közvetítő végkészülék, mint hívást kezdeményező egység, a 20 információ közvetítő végkészülék pedig, mint hívott egység szerepel, de az eszközkészlet több jeltovábbító összeköttetés egyidejű létesítésére, u.n. „konferencia-kapcsolat” megvalósítására is értelemszerűen alkalmas.

A 10 információ közvetítő végkészüléken a hívandó 20 információ közvetítő végkészülék egyedi azonosító számát, pl. telefonszámát, vagy éppen a 20 információ közvetítő végkészülék 22a készülékazonosító jelzését tárcsázva, bejelentkezését a 30 információ továbbító hálózaton keresztül úgy juttatja el a 40 központi forgalomkoordináló egységhez, hogy a bejelentkező üzenetet a 10 információ közvetítő végkészülék 13 C-regiszterében lévő 41a mester-kódoló kulcs segítségével kódolja, és az így kódolt jelzést a 18 küldő részegységen át továbbítja a 40 központi forgalomkoordináló egységhez.

A 40 központi forgalomkoordináló egység a 41a mester-kódoló kulccsal titkosított üzenetet a 42 MD-regiszterében rögzített 42a mester-dekódoló kulcs segítségével visszafejti. Az üzenet tartalma alapján egyfelől azonosítja a 10 információ közvetítő végkészüléket annak saját 12a készülékazonosító jelzése alapján, másfelől ellenőrzi, hogy a kapott 22a készülékazonosító jelzéshez tartozik-e ténylegesen 20 információ közvetítő végkészülék vagy sem, és ha igen, akkor a 22a készülékazonosító jelzés szerint kikeresi a 43 memóriaegység 43b alaprekeszéből a 20 információ közvetítő végkészülék 26 kódoló kulcsát. A 40 központi forgalomkoordináló egység a 20 információ közvetítő végkészülékének 26 kódoló kulcsát a 10 információ közvetítő végkészülék 16 kódoló kulcsának segítségével titkosítja, és így küldi azt tovább a 10 információ közvetítő végkészülék 19 fogadó részegységéhez. A 10 információ közvetítő végkészülék 19 fogadó részegysége a kapott információt saját 17 dekódoló kulcsa segítségével visszafejti és ezáltal időlegesen hozzájut a 20 információ közvetítő végkészülék 26 kódoló kulcsához, amelyet a 10 információ közvetítő végkészülék 15 átmeneti tároló regiszterében raktároz.

A hívást kezdeményező 10 információ közvetítő végkészülék a 30 információ továbbító hálózaton keresztül megpróbálja elérni a 20 információ közvetítő végkészüléket. Ha a 10 információ közvetítő végkészülék nem képes elérni a 22a készülékazonosító jelzéshez tartozó 20 információ közvetítő végkészüléket, akkor a kapcsolatfelvétel nem jöhet létre.

Abban az esetben, ha a 10 információ közvetítő végkészülék elérte a 20 információ közvetítő végkészüléket, akkor a 10 információ közvetítő végkészülék 26 kódoló kulcsával titkosított módon elküldi saját 12a készülékazonosító jelzését a 20 információ közvetítő végkészüléknek. A 20 információ közvetítő végkészülék ezt visszafejti saját 27 dekódoló kulcsával és ezt követően a 40 központi forgalomkoordináló egységhez tartozó 41a mester-kódoló kulcs segítségével kódolva elküldi azt a 30 információ továbbító hálózaton keresztül a 40 központi forgalomkoordináló egységhez, és kéri attól a 10 információ közvetítő végkészülék 16 kódoló kulcsát.

A 40 központi forgalomkoordináló egység a 20 információ közvetítő végkészüléktől kapott 12a készülékazonosító jelzésnek megfelelően a 43 memóriaegység 43a alaprekeszéből kiválasztja a 10 információ közvetítő végkészülék 16 kódoló kulcsát. Ezt követően a 40 központi forgalomkoordináló egység a 10 információ közvetítő végkészülék 16 kódoló kulcsát a 20 információ közvetítő végkészülék 26 kódoló kulcsa segítségével titkosítja, és így küldi tovább a 20 információ közvetítő végkészüléknek. A 40 központi forgalomkoordináló egységtől kapott titkosított üzenetet a 20 információ közvetítő végkészülék 29 fogadó részegységében fogadja, saját 27 dekódoló kulcsával visszafejti, aminek következtében megtudja a hívást kezdeményező 10 információ közvetítő végkészülék 16 kódoló kulcsát, amit a 20 információ közvetítő végkészülék 25 átmeneti tároló regiszterében kiolvashatatlan módon időlegesen eltárol.

A 16 kódoló kulcsnak a 20 információ közvetítő végkészülék részére, míg a 26 kódoló kulcsnak a 10 információ közvetítő végkészülék részére történő megküldése után a 10 információ közvetítő végkészülék képes arra, hogy a 20 információ közvetítő végkészülékkel közlendő információit a 26 kódoló kulcs segítségével úgy titkosítsa, hogy azokat a 18 küldő részegységen már egyenesen a 20 információ közvetítő végkészülékhez lehessen eljuttatni, amely a 30 információ továbbító hálózaton át a 10 információ közvetítő végkészülék 18 küldő részegységétől kapott -, és a 20 információ közvetítő végkészülék 26 kódoló kulcsával kódolt - adatokat 29 fogadó részegységében fogadva saját 27 dekódoló kulcsával visszafejtheti, és az így egyszerűen értelmezhetővé válik a 20 információ közvetítő végkészüléket használó személy, vagy éppen berendezés számára.

A 10 információ közvetítő végkészüléktől kapott információkra a 20 információ közvetítő végkészülék úgy tud válaszolni, hogy az általa küldeni kívánt adatokat a 25 átmeneti tároló regiszterben lévő 16 kódoló kulcs segítségével titkosítja, és a 28 küldő részegységbe, onnan pedig a 30 információ továbbító hálózatba küldve közvetlenül a 10 információ közvetítő végkészülék 19 fogadó részegységéhez továbbítja. A 19 fogadó részegységre érkező adatokat a 10 információ közvetítő végkészülék 17 dekódoló kulcsával próbálja meg visszafejteni, és ha ez sikerült, akkor az már a 10 információ közvetítő végkészüléket használó személy, vagy berendezés számára egyszerűen értelmezhető.

Ezen közvetlen, a 10 információ közvetítő végkészülék és a 20 információ közvetítő végkészülék közötti jelforgalom a 30 információ továbbító hálózaton keresztül már úgy bonyolódik, hogy abban a 40 központi forgalomkoordináló egység nem vesz részt. A 10 információ közvetítő végkészülék és a 20 információ közvetítő végkészülék ideiglenesen megismerve a másik 16 kódoló kulcsát, illetőleg

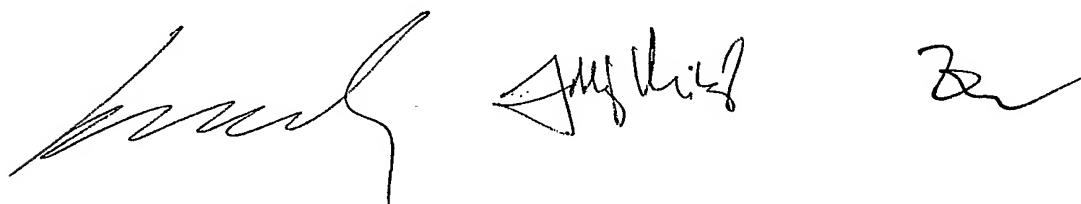
26 kódoló kulcsát képes a közvetlen információcserére. A 10 információ közvetítő végkészülék és a 20 információ közvetítő végkészülék közötti forgalom megszűnése után a 10 információ közvetítő végkészülék 15 átmeneti tároló regiszterében lévő 26 kódoló kulcs kitörlődik, és ugyanez történik a 20 információ közvetítő végkészülék 25 átmeneti tároló regiszterében lévő 16 kódoló kulccsal is.

A 10 információ közvetítő végkészülék hívásának befejezése után a 20 információ közvetítő végkészülékben ismét csak a 24 D-regiszterben lévő saját 27 dekódoló kulcs, valamint a 23 C-regiszterben található 41a mester-kódoló kulcs marad. A 10 információ közvetítő végkészülék pedig a 14 D-regiszterben lévő saját 17 dekódoló kulcsa mellett csak a 13 C-regiszterben lévő 41a mester-kódoló kulcsot őrzi meg.

A folyamat ismertetése alapján belátható, hogy a 10 információ közvetítő végkészülék, a 20 információ közvetítő végkészülék, és a 40 központi forgalomkoordináló egység az adatközlítés felépítése és a forgalmazása során egyetlen pillanatra sem kerül olyan helyzetbe, hogy egyszerre rendelkezzen valamely összetartozó kódoló-dekódoló kulcs-párral. Nincs tehát mód arra, hogy a 16 kódoló kulcs - 17 dekódoló kulcs, vagy a 26 kódoló kulcs - 27 dekódoló kulcs egyszerre legyen hozzáférhető bárki számára az eszközkészlet használói közül.

Magától értetődő, hogy a 40 központi forgalomkoordináló egység a 30 információ továbbító hálózat jellemzői által meghatározott, a hálózati eléréshez szükséges hálózati címeket is képes tárolni és adminisztrálni, valamint a 10 és 20 információ közvetítő végkészülékek felé a kapcsolat felépítéséhez szükséges címeket továbbítani.

A biztonság további növelése érdekében az is megoldható, hogy a 40 központi forgalomkoordináló egység se tartalmazza egyszerre a 41a mester-kódoló kulcsot és a 42a mester-dekódoló kulcsot. A megfelelő kódoló-dekódoló kulcs-párok csak egyik tagjának ismerete pedig lehetetlenné teszi a titkosított üzenetek megfejtését.



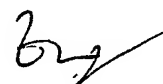
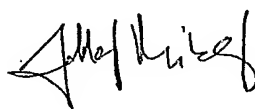
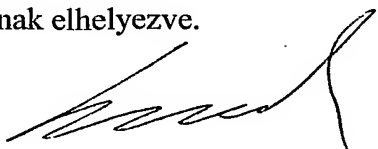
SZABADALMI IGÉNYPONTOK

1. Eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására, amely információ továbbító hálózattal történő együttműködésre alkalmas, az információ-forgalomban résztvevő információ közvetítő végkészülékeket tartalmaz, az egyes információ közvetítő végkészülékek küldő részegységgel és fogadó részegységgel, valamint készülékazonosító jelzést tartalmazó ID-regisztert, kódoló kulcs tárolására alkalmas C-regisztert és dekódoló kulcs tárolására alkalmas D-regisztert magukban foglaló tároló részegységgel vannak ellátva, ahol a kódoló kulcsot tartalmazó C-regiszter a küldő részegységgel van összeköttetésben, az egyes információ közvetítő végkészülékekhez pedig kódoló kulcs és azzal együttműködő dekódoló kulcs van hozzárendelve, azzal **jellemezve**, hogy minden egyes információ közvetítő végkészülék (10) tároló részegysége (11) más információ közvetítő végkészülékek (20) kódoló kulcsainak (26) ideiglenes tárolására szolgáló egy vagy több átmeneti tároló regiszterrel (15), míg az információ továbbító hálózat (30) legalább egy központi forgalomkoordináló egységgel (40) van kiegészítve, a központi forgalomkoordináló egységnek (40) mester-dekódoló kulcsot (42a) tároló MD-regisztere (42), valamint az egyes információ közvetítő végkészülékekhez (10, 20) tartozó kódoló kulcsok (16, 26) tárolására szolgáló alapekeszeket (43a, 43b) tartalmazó memóriaegysége' (43) van, továbbá a központi forgalomkoordináló egységhez (40) a mester-dekódoló kulccsal (42a) együttműködő mester-kódoló kulcs (41a) van hozzárendelve, az információ közvetítő végkészülékek (10, 20) C-regiszterei (13a, 23a) pedig a központi forgalomkoordináló egység (40) MD-regiszterében (42) tárolt mester-dekódoló kulccsal (42a) együttműködő mester-kódoló kulccsal (41a) vannak ellátva.

2. Az 1. igénypont szerinti eszközkészlet, azzal **jellemezve**, hogy az információ közvetítő végkészülékek (10, 20) átmeneti tároló regiszterei (15, 25) a küldő részegységgel (18, 28) vannak kapcsolatban.

3. Az 1. vagy a 2. igénypont szerinti eszközkészlet, azzal **jellemezve**, hogy a központi forgalomkoordináló egység (40) mester-kódoló kulcsot (41a) tároló MC-regiszterrel (41) van ellátva.

4. Az 1. - 3. igénypontok bármelyike szerinti eszközkészlet, azzal **jellemezve**, hogy az egyes információ közvetítő végkészülékek (10, 20) tároló részegységében (11, 21) csak az adott információ közvetítő végkészülék (10, 20,) saját kódoló kulcsától (16, 26) mentes információk vannak elhelyezve.



Hivatkozási jelek jegyzéke

10 információ közvetítő végkészülék

11 tároló részegység
12 ID-regiszter
12a készülékazonosító jelzés
13 C-regiszter
14 D-regiszter
15 átmeneti tároló regiszter
16 kódoló kulcs
17 dekódoló kulcs
18 küldő részegység
19 fogadó részegység

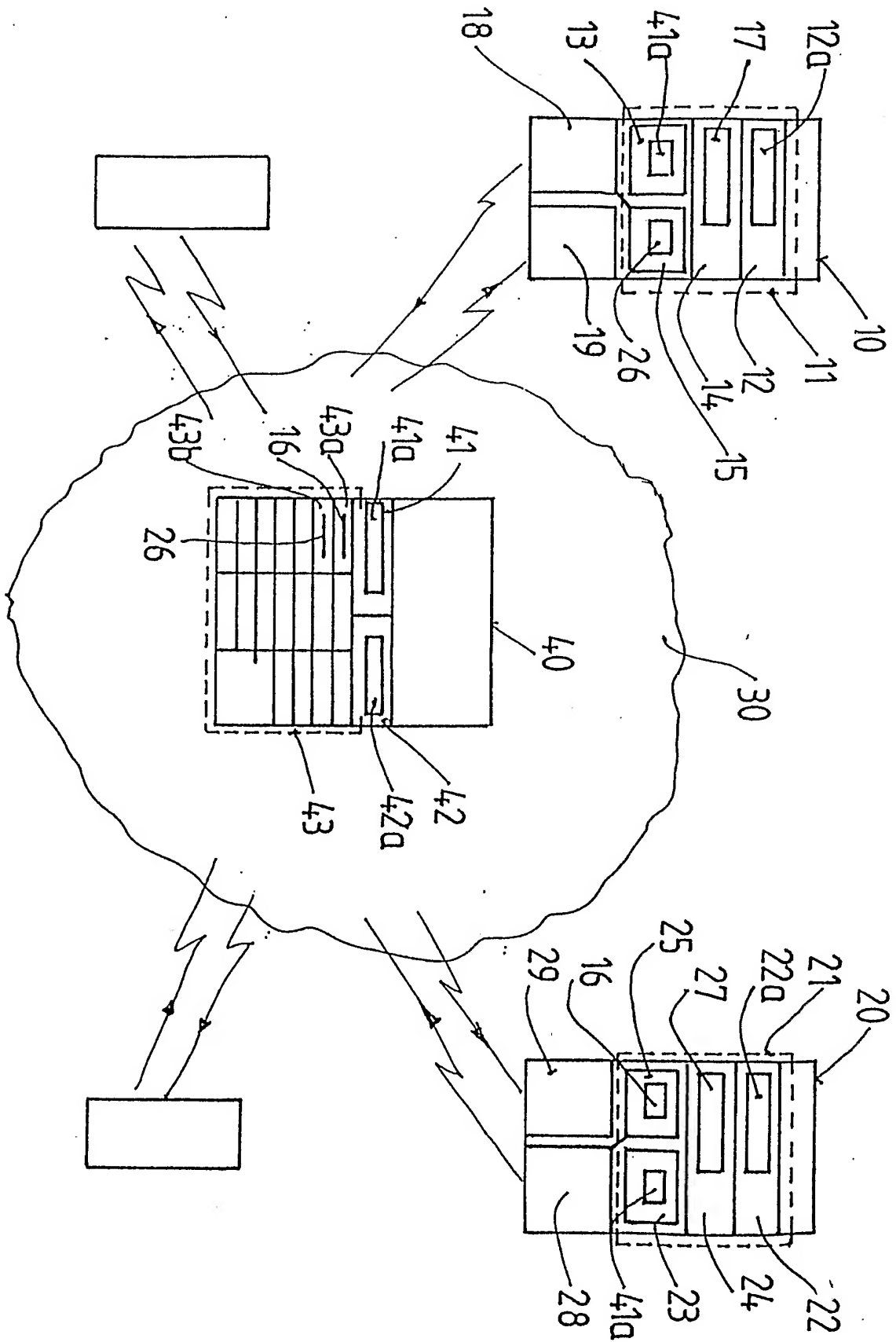
20 információ közvetítő végkészülék

21 tároló részegység
22 ID-regiszter
22a készülékazonosító jelzés
23 C-regiszter
24 D-regiszter
25 átmeneti tároló regiszter
26 kódoló kulcs
27 dekódoló kulcs
28 küldő részegység
29 fogadó részegység

30 információ továbbító hálózat

40 központi forgalomkoordináló egység

41 MC-regiszter
41a mester-kódoló kulcs
42 MD-regiszter
42a mester-dekódoló kulcs
43 memóriaegység
43a alaprekesz
43b alaprekesz



1. ábra

Handwritten signature and date: 2009. 11. 11.

Eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására

A bejelentő

JOBÁGY Miklós, Kecskemét, HU,

KUTI Gábor, Jászberény, HU,

ZELENÁK János, Budapest, HU

A bejelentés napja: 2004. 03. 01.

A találmány tárgya eszközkészlet közvetlen információ-forgalom Interneten keresztül történő biztonságos lebonyolítására, amely az információ-forgalomban résztvevő információ közvetítő végkészülékeket, valamint az információ közvetítő végkészülékeket egymással összekötő információ továbbító hálózatot tartalmaz, az egyes információ közvetítő végkészülékek küldő részegységgel és fogadó részegységgel, valamint készülékazonosító jelzést tartalmazó ID-regisztert, kódoló kulcs tárolására alkalmas C-regisztert és dekódoló kulcs tárolására alkalmas D-regisztert magukban foglaló tároló részegységgel vannak ellátva, ahol a kódoló kulcsot tartalmazó C-regiszter a küldő részegységgel van összeköttetésben, az egyes információ közvetítő végkészülékekhez pedig kódoló kulcs és azzal együttműködő dekódoló kulcs van hozzárendelve.

A találmány jellegzetessége, hogy minden egyes információ közvetítő végkészülék (10) tároló részegysége (11) más információ közvetítő végkészülékek (20) kódoló kulcsainak (26) ideiglenes tárolására szolgáló egy vagy több átmeneti tároló regiszterrel (15), míg az információ továbbító hálózat (30) legalább egy központi forgalomkoordináló egységgel (40) van kiegészítve, a központi forgalomkoordináló egységnek (40) mester-dekódoló kulcsot (42a) tároló MD-regisztere (42), valamint az egyes információ közvetítő végkészülékekhez (10, 20) tartozó kódoló kulcsok (16, 26) tárolására szolgáló alaprekeszeket (43a, 43b) tartalmazó memóriaegysége (43) van, továbbá a központi forgalomkoordináló egységhez (40) a mester-dekódoló kulccsal (42a) együttműködő mester-kódoló kulcs (41a) van hozzárendelve, az információ közvetítő végkészülékek (10, 20) C-regiszterei (13a, 23a) pedig a központi forgalomkoordináló egység (40) MD-regiszterében (42) tárolt mester-dekódoló kulccsal (42a) együttműködő mester-kódoló kulccsal (41a) vannak ellátva.

A jellemző ábra: 1. ábra

